# INTERNET EST-IL RÉELLEMENT CONTRÔLÉ PAR 14 PERSONNES QUI DÉTIENNENT 7 CLÉS SECRÈTES ?

Dès les années cinquante, les ordinateurs ont été mis en réseau pour échanger des informations, conduisant à la naissance d'Internet en 1983, puis du Web en 1989. Mais qui contrôle aujourd'hui ce formidable outil ?
Une simple requête sur un moteur de recherche nous apprend qu'Internet « *est en réalité contrôlé par 14 personnes qui détiennent 7 clés secrètes* »[1]. Les sites relayant cette information surprenante sont nombreux : « *Paul Kane, a computer expert, is one of only seven people around the world to be given responsibility for rebooting the internet in the event of a catastrophe* »[2] ; « *Cette Suédoise détient la clé d'Internet ! Quatorze personnes dans le monde protègent les clés de chiffrement du système des adresses internet. Rencontre avec l'une d'entre elles, à Stockholm.* »[3] ; etc[4].
Qu'en est-il vraiment ?

La « véritable » adresse du site Web qui a pour URL https://www.mathemathieu.fr est une adresse numérique[5] : 83.229.19.69. En effet, comme il est plus facile de retenir une suite de lettres que de chiffres[6], un service d'annuaire distribué dans le monde entier permet de traduire les noms de domaine en adresses IP : c'est **le système DNS** (Domain Name System).
Ce système DNS est organisé sous la forme d'une base de données répartie et hiérarchisée. Outre la racine de la hiérarchie qui se présente par un point « . », il existe les domaines de plus haut niveau, aussi connus sous l'acronyme TLD (Top Level Domain). Les plus populaires sont . COM, . ORG,. NET, . FR, etc[7].

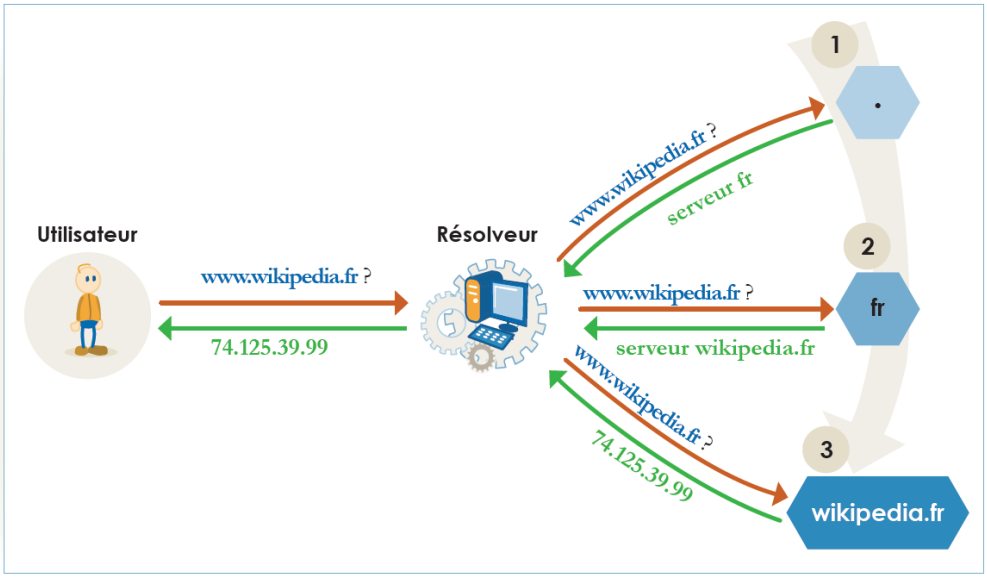


Figure 1: Source : AFNIC

Les serveurs responsables de la racine de la hiérarchie sont appelés ***serveurs racines*** ou ***serveurs root*** : on lit souvent qu'il en existe 13… Il y a bien 13 « root name servers » mais il s'agit en réalité de 13 « identités

1 https://dailygeekshow.com/internet-sept-cles/

2 https://www.telegraph.co.uk/technology/internet/7914153/Briton-holds-key-to-the-internet.html

3 https://www.lepoint.fr/high-tech-internet/cette-suedoise-detient-la-cle-d-internet-28-05-2013-1672821_47.php

4 cheminerverslaverite.over-blog.com ; www.tuxboard.com ; www.atlantico.fr ; www.parismatch.com ; etc.

5 Au 18 avril 2023.

6 Outre le fait qu'il est plus facile pour un humain de retenir « www.certa.ssi.gouv.fr » que 213.56.176.2, ceci permet au gestionnaire du site de modifier son adresse IP (changement de fournisseur d'accès, par exemple) en ayant juste à mettre à jour le serveur DNS plutôt que d'avoir à informer tous les clients potentiels de la nouvelle adresse IP.

7 On distingue généralement parmi les TLDs ceux attribués en fonction des pays comme .FR, les ccTLDs (country code TLDs), et ceux plus génériques, les gTLDs, comme .COM, .NET ou .ORG.

de serveur » (serveurs A, B, C, … , M) ayant chacun une adresse IP[8] ; les serveurs racines sont donc un réseau de milliers de serveurs dans de nombreux pays à travers le monde – 1 698 serveurs[9] au 18 avril 2023, répartis sur 1 488 sites – et chacun est une copie du véritable serveur maître à partir duquel les copies sont effectuées ; le véritable serveur maître à partir duquel les copies sont effectuées n'est pas l'un des serveurs racines publics).

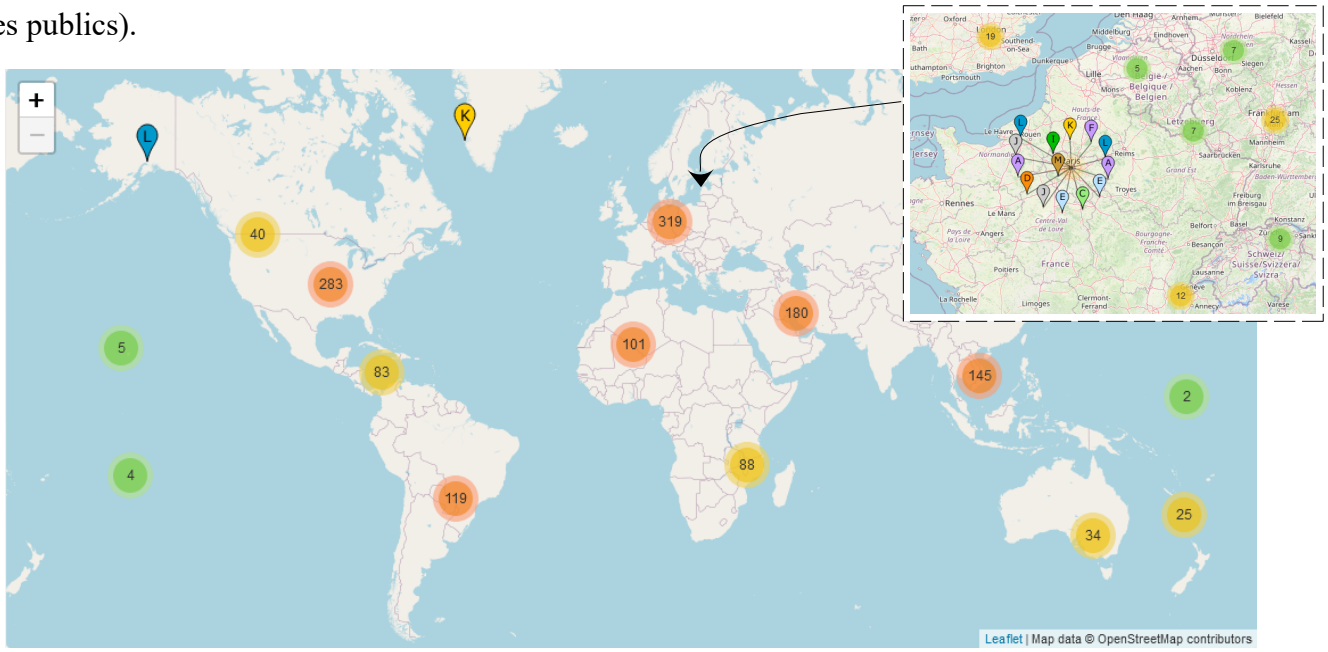



Figure 2: Source : root-servers.org (en zoomant, les localisations des instances se précisent)

Douze organisations contrôlent ces serveurs, deux sont européennes, une japonaise, les autres étant américaines. Ces serveurs ne sont pas de simples machines mais correspondent à plusieurs installations réparties dans des lieux géographiques divers.

Par exemple, la racine « C » est contrôlée par *Cogent Communications* (opérateur de télécommunications multinational américain) et elle est constituée de 12 serveurs situés sur 12 sites :

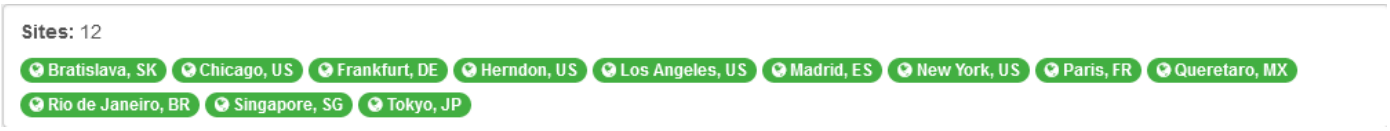



Figure 3: Source : root-servers.org

Le résolveur DNS garde en mémoire les résultats : si on cherche deux fois le même nom de domaine, le résolveur de mon fournisseur d'accès à internet répondra très vite la seconde fois, car il garde en mémoire le résultat pendant environ deux jours (la liste des serveurs racines étant gardée en cache pendant 6 jours). La durée de cette mémoire dépend du TTL (*Time To Live*), qui peut être différent pour chaque nom de domaine. Voilà pourquoi, lorsqu'on change d'hébergeur (du nom de domaine), cela peut mettre jusqu'à 2 jours, le temps que les caches soient actualisés.

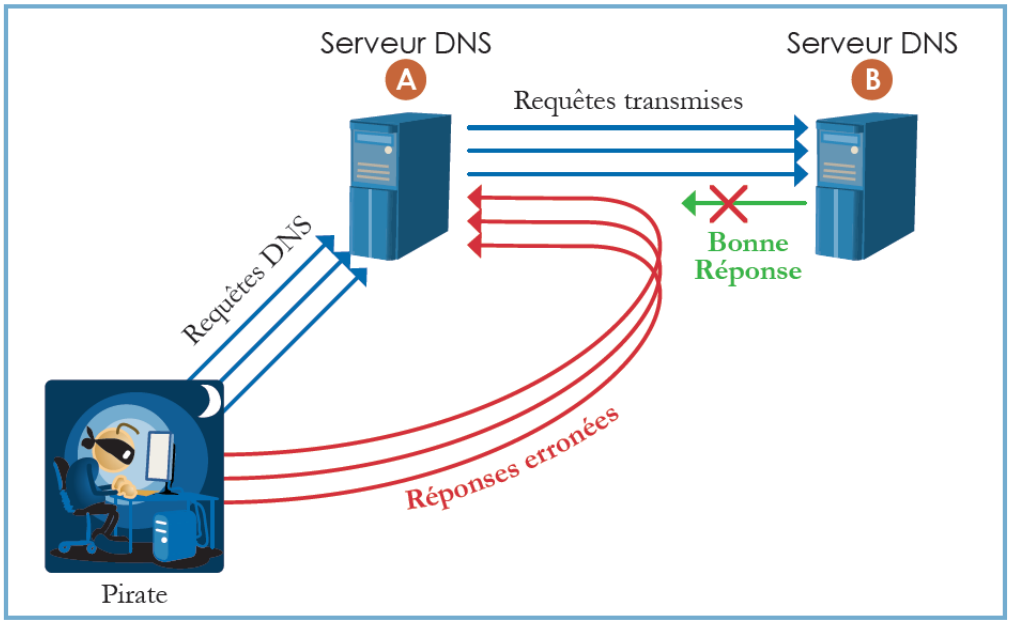
Si l'un des *root servers* ne répond plus, la charge est répartie entre les serveurs qui subsistent. Si aucun d'entre eux ne pouvait répondre aux requêtes, les noms de domaines deviendraient progressivement inaccessibles, au fur et à mesure que les informations dans les caches parviendraient à expiration. L'adresse exacte de la plupart des serveurs n'est pas publiée pour éviter les attaques ciblées.

8 La liste de ces 13 adresses IP et leurs opérateurs est disponible ici : https://www.iana.org/domains/root/servers.

9 Il y avait 130 sites en 2007. Pour voir la liste actualisée de ces sites : https://root-servers.org/.

Au fur et à mesure, **le système DNS est devenu vulnérable aux attaques**.
L'AFNIC en recense[10] six grandes familles, les trois principales étant :

• l'empoisonnement du cache (ou ***cache poisoning***) qui vise à intoxiquer le résolveur pour qu'il considère que le serveur « pirate » est légitime, en lieu et place du serveur originel. Cette opération permet notamment de capter et de détourner les requêtes vers un autre site web sans que les utilisateurs puissent s'en rendre compte, avec le risque de les voir confier des données personnelles en se croyant sur le site légitime de la victime de l'attaque : c'est ce qu'on appelle le *pharming*.




Les attaques par empoisonnement de cache

Figure 4: Source : AFNIC

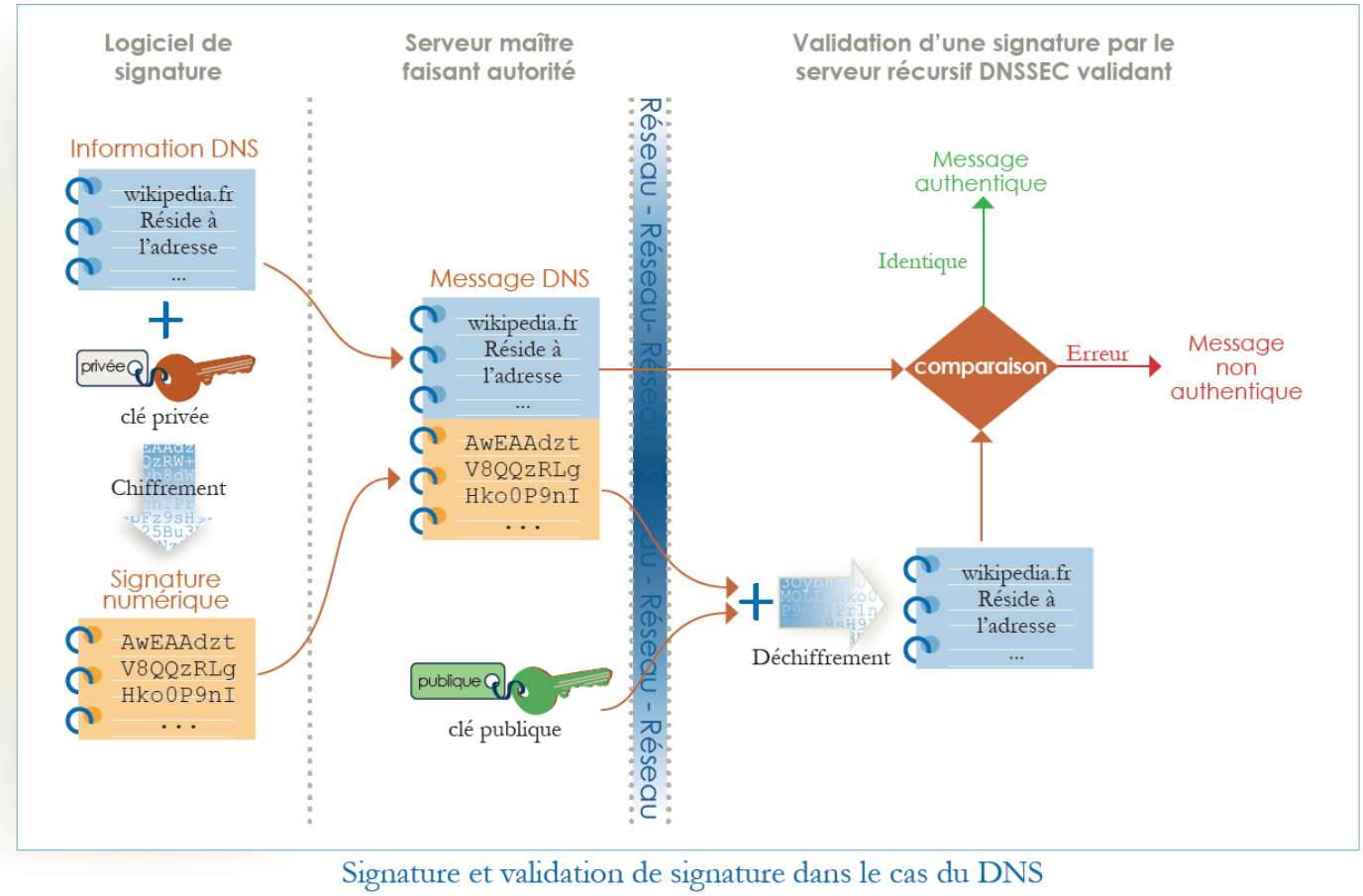
• le déni de service (***Denial of Service*** ou DoS) qui a pour objectif de rendre l'accès à un service impossible ou très pénible. Cette attaque peut se faire de manière brutale (saturation des serveurs par envoi massif de requêtes simultanées) ou plus subtile si l'attaquant essaie d'épuiser une ressource rare sur le serveur.
Par exemple, le 30 novembre 2015 (pendant presque trois heures) et le 1er décembre 2015 (pendant une heure), les 13 identités de serveurs racines ont fait l'objet de deux attaques DoS, causant des délais d'attente sur les serveurs racines B, C, G et H. Environ 5 millions de requêtes ont été envoyées par seconde vers les serveurs avec deux domaines uniques à l'origine de l'attaque, un pour chaque attaque. Trois des treize serveurs racines ont subi des ralentissements, mais l'impact sur l'ensemble d'internet est resté limité.

• le déni de service distribué (***distributed Denial of Service*** ou dDoS), forme élaborée du DoS impliquant plusieurs milliers d'ordinateurs, en général dans le contexte d'un réseau d'ordinateurs « zombies » dont l'attaquant se sert à l'insu de leurs propriétaires grâce à des programmes malveillants diffusés via des vers se propageant d'une machine à l'autre.
Par exemple, le 21 octobre 2016, dDoS de plus d'un téraoctet par seconde visant le service *Dyn Managed DNS*. De nombreux sites qui utilisent ce service, tels que Twitter, Ebay, Netflix, GitHub, PayPal, sont inaccessibles pendant une dizaine d'heures. Les attaquants se sont servis d'objets connectés piratés (comme des caméras de surveillance) infectés par le logiciel malveillant nommé Mirai pour relayer le flux de paquets massif.

10 https://www.afnic.fr/wp-media/uploads/2021/01/DNS-types-dattaques-et-techniques-de-se%CC%81curisation.pdf

L'utilisation du protocole HTTPS est très utile, mais ne permet pas de se protéger contre ce type d'attaques : **la protection la plus efficace est l'utilisation du protocole DNSSEC** (DNS sécurisé).

DNSSEC fonctionne en signant numériquement chaque enregistrement DNS afin que toute falsification de cet enregistrement puisse être détectée. Cette signature repose sur un algorithme de chiffrement asymétrique, c'est-à-dire qui utilise une paire de clés cryptographiques ayant des rôles complémentaires : la première clé, privée, signe par chiffrement alors que la seconde clé, publique, vérifie les signatures par déchiffrement (c'est pourquoi on appelle souvent cette clé publique « clé de signature »).

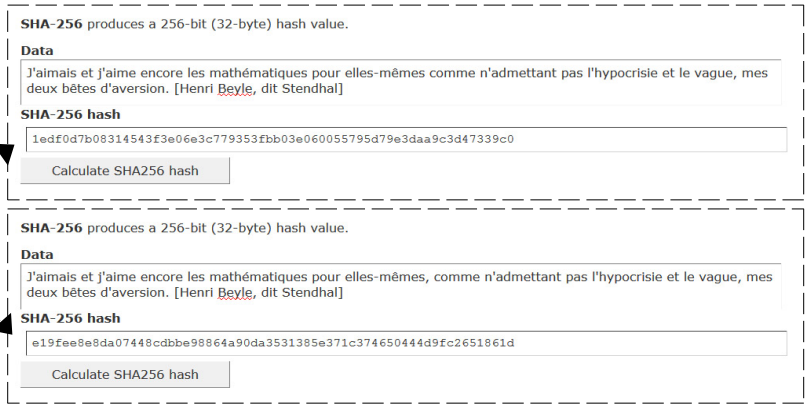


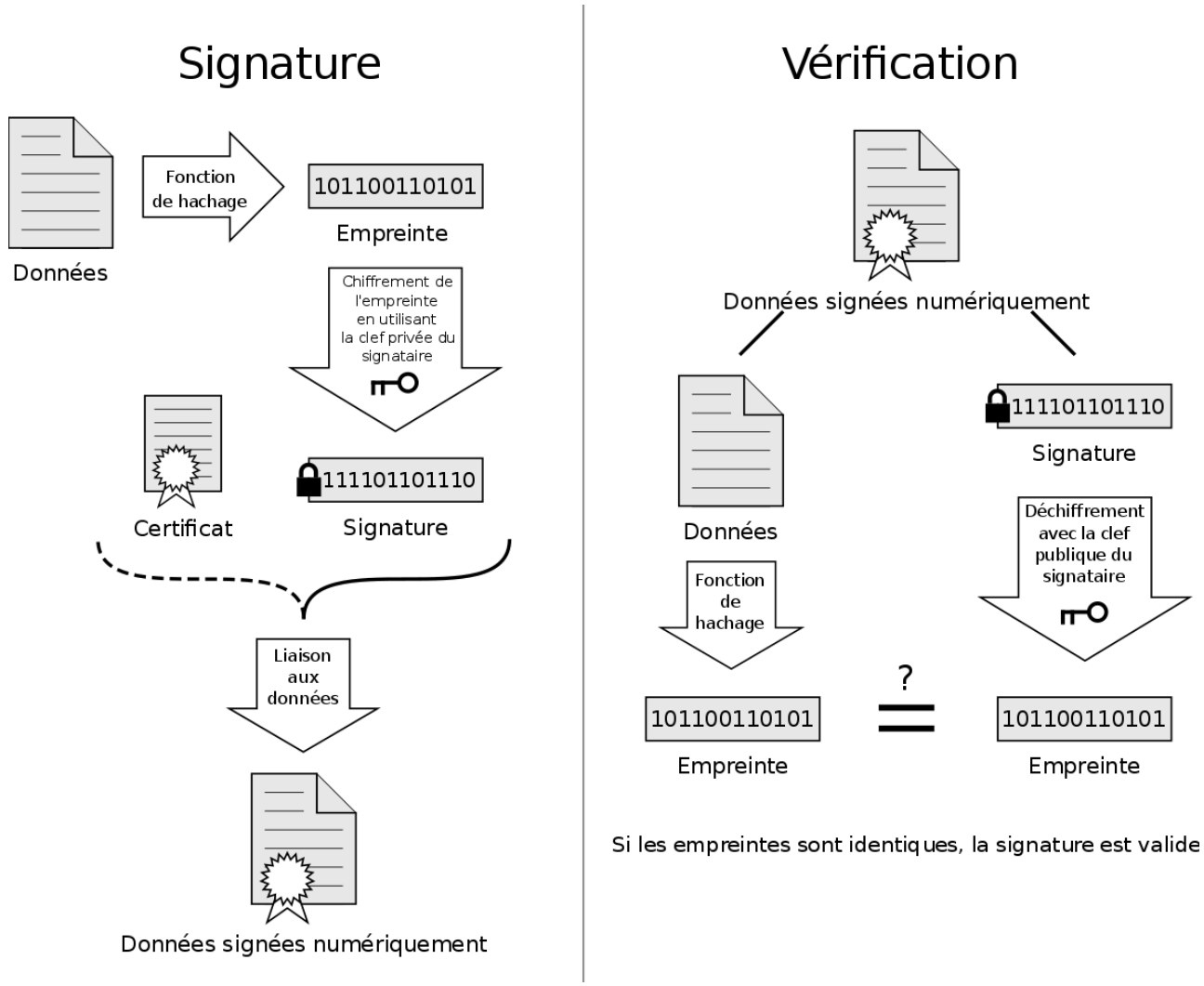

Signature et validation de signature dans le cas du DNS

Figure 5: Source : AFNIC

En réalité, chiffrer un message est souvent long et coûteux en ressources, c'est pourquoi on préfère chiffrer une empreinte (appelé un *hash*) du message ou du fichier à transmettre : ce *hash* est en quelque sorte un résumé du message, très sensible au moindre changement (empreintes très différentes pour des données quasi identiques*).

* Un des algorithmes de *hash* le plus utilisé est SHA-256 (*Secure Hash Algorithm 256 bits*).
Cette fonction a été conçue par la *National Security Agency* des États-Unis (NSA).
Ici on voit clairement que les *hash* de deux phrases qui diffèrent d'une simple virgule sont très différents (ces *hash* sont ici codés en hexadécimal).






Le certificat électronique (délivré par une autorité de certification) associe une clé privée à une personne / machine, puisqu'il est remis à une personne physique après vérification des documents justificatifs et de l'identité de la personne. C'est donc une véritable carte d'identité numérique.

*Avant de continuer, précisons que DNSSEC n'a, par exemple, pas vocation à chiffrer les enregistrements DNS, ni à assurer la confidentialité des échanges sur le réseau, ni à garantir la sécurité d'une transaction comme le font les certificats SSL. Il ne protège pas contre le phishing*[11] *ou le vol de noms de domaine, contre les virus et autres techniques d'infection des postes informatiques, ou encore contre les attaques visant les sites web eux-mêmes*[12].

11 L'hameçonnage (*phishing* en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, etc. Le but recherché est de voler des informations personnelles ou professionnelles (comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

12 http://www.afnic.fr/medias/documents/afnic-dossier-dnssec-2010-09.pdf

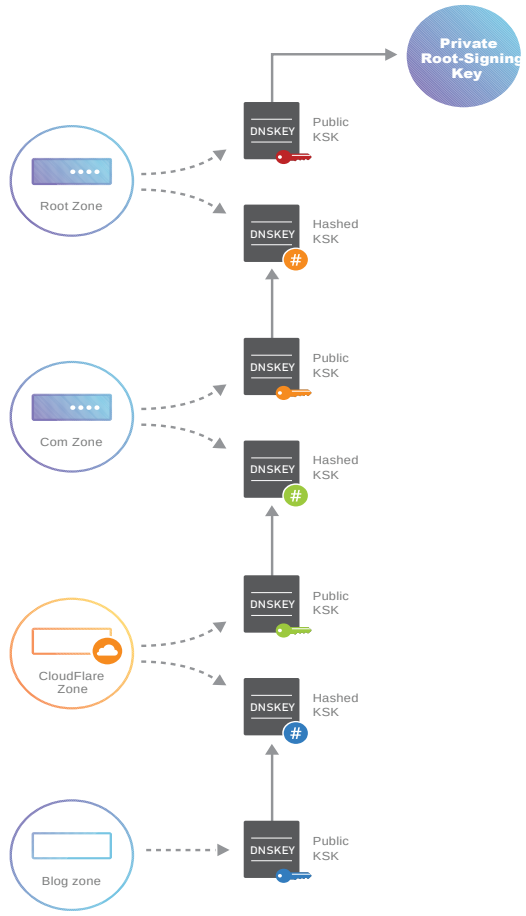



Figure 6: Source : Cloudflare KSK = Key Signing Key

← Les clés de chaque couche de la hiérarchie DNS sont signées par des clés de la couche précédente qui les garantissent efficacement, tout comme les noms de domaines sont délégués d'une couche à la suivante. Cette « chaîne de confiance » est utilisée pour valider les signatures numériques accompagnant les enregistrements protégés DNSSEC afin de détecter les modifications[13].

La clé publique n'est pas signée par la clé privée de la zone mais par la clé privée de la zone mère. Par exemple, la clé publique de la zone `cloudflare.com` est signée par la zone `com`.
Chaque clé publique d'une zone est signée par sa zone mère (créant ainsi la « chaîne de confiance ») sauf celle de la zone racine : elle n'a pas de zone mère chargée de signer sa clé !

**Les clés de la zone racine** (Root zone Key Signing Key = RKSK) **constituent donc un important point de départ pour la validation des données DNS.**

Si un résolveur fait confiance à la clé publique de la zone racine, il peut faire confiance aux clés publiques des zones de premier niveau signées par la clé privée de la racine, telle que la clé publique de la zone `com`. Et comme le résolveur peut faire confiance à la clé publique de la zone `com`, il peut faire confiance aux clés publiques qui ont été signées par leur clé privée respective, telles que la clé publique de `cloudflare.com`[14].
Il fallait donc confier les clés cryptographiques de la racine DNS à un organisme de confiance : l'ICANN.

## ICANN (Internet Corporation for Assigned Names and Numbers)

Société de droit californien à but non lucratif ayant pour principales missions d'administrer les ressources numériques d'Internet, telles que l'adressage IP et les noms de domaines de premier niveau (TLD), et de coordonner les acteurs techniques.
Comme elle le précise elle-même, l'ICANN « n'a aucun contrôle sur le contenu publié sur Internet. Elle ne peut mettre fin aux spams et ne gère aucunement l'accès à Internet. Mais de par le rôle de coordination qu'elle joue au sein du système d'attribution de noms Internet, elle exerce une influence non négligeable sur le développement et l'évolution d'Internet. »
En 2016, les États-Unis, sous pression internationale (de l'UE, de nombreux pays d'Asie et d'Amérique du Sud), ont renoncé à des décennies de gérance du DNS racine via l'organisme ICANN qui était rattaché au *Département du Commerce* de l'administration américaine et est désormais placé entre les mains d'une organisation internationale.

**C'est pourquoi a lieu chaque trimestre, depuis 2010, une cérémonie des clés !**
Il s'agit d'une procédure rigoureuse permettant notamment de créer les clés de la zone DNS racine pour les trois prochains mois (ces clés changent automatiquement tous les 15 à 16 jours).

13 https://www.icann.org/resources/pages/dnssec-2012-02-25-en

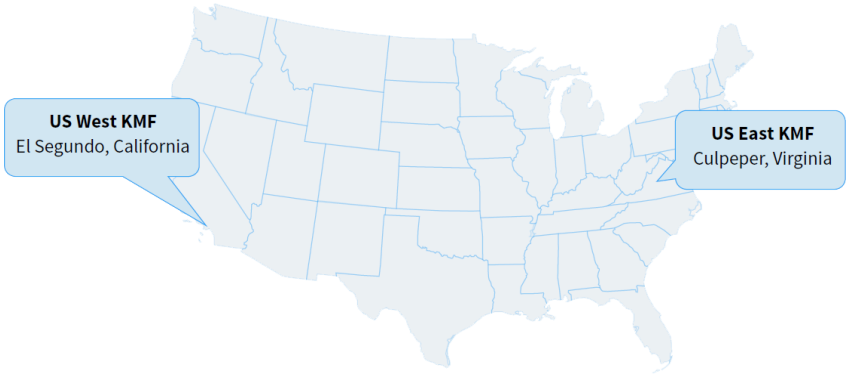
14 Dans la pratique, la zone mère ne signe pas directement la clé de la zone enfant, le mécanisme est plus complexe mais l'idée reste la même. Si cela vous intéresse, voir Cloudflare, AFNIC, ThousandEyes et HSR.

**Les clés (clé publique et clé privée) utilisées dans ce processus sont** donc, pour un temps, **les clés de l'ensemble de l'Internet protégé par DNSSEC**[15].

Une ou plusieurs personnes détiennent-elles cette clé ? Ces personnes contrôlent-elles alors Internet ?!
Comme souvent, l'histoire de « 14 personnes qui contrôlent Internet » est un peu vraie, un peu fausse… mais nous allons voir qu'il s'agit d'un titre racoleur plutôt mensonger, tout comme les articles qui diffusent cette idée.

Tout d'abord, **cette cérémonie est publique**, auditée, contrôlée, et même diffusée en direct (streaming).

Ces clés cryptographiques sont conservées dans **deux installations sécurisées** (*key management facilities* = KMF) **distantes de plus de 4 000 kilomètres** : El Segundo (W) en Californie et Culpeper (E) en Virginie. La cérémonie alterne entre ces deux lieux.




Les clés sont protégées par plusieurs couches de sécurité physique telles que des gardes de bâtiment, des caméras, des scanners biométriques et rétiniens, des cages surveillées et des coffres-forts.

La couche la plus interne de sécurité physique est un appareil spécialisé appelé module de sécurité matérielle (*Hardware Safe Controller* = **HSM**), qui stocke les clés cryptographiques réelles.
Un HSM résiste à la falsification physique : par exemple, si quelqu'un tente d'ouvrir le périphérique ou le laisse tomber, le HSM efface toutes les clés qu'il stocke.

L'ICANN conserve **deux HSM dans chaque établissement** (au cas où un HSM dysfonctionnerait).
La clé cryptographique privée de la zone racine ne peut pas être utilisée en dehors d'un HSM et le système conçu pour faire fonctionner un HSM nécessite la présence de nombreuses personnes. Certaines de ces personnes sont des membres de la communauté technique, appelés représentants de la communauté de confiance (*Trusted Community Representative* = **TCR**), et d'autres font partie du personnel de l'ICANN. Chaque personne a un rôle spécifique dans l'activation du HSM.
Ces TCRs sont donc des personnes reconnues auprès de la communauté Internet ; des personnes considérées comme directement affiliées au processus de gestion de la zone racine (par exemple des salariés de l'ICANN ou de Verisign) ne peuvent pas devenir des TCRs. La démission volontaire est bien sûr possible (mais encadrée) et les TCRs actifs depuis plus de cinq ans sont éligibles à une retraite obligatoire[16].
Il existe trois types de TCR :

– l'agent de cryptographie (***Cryptography Officer*** = **CO**)
Il assiste 1 à 2 fois par an à la cérémonie de signature des clés, en apportant une clé (traditionnelle, en métal) qui ouvrira un coffre-fort qui lui-même contiendra des cartes à puces, dont une permettant d'activer le HSM.
Tout en assistant aux cérémonies, les CO assistent à la cérémonie et la commentent, attestant à la communauté dans son ensemble que les cérémonies ont été menées de manière appropriée.
Entre les cérémonies, ils sont responsables de garder leur clé en sécurité.

15 En réalité, la RKSK n'est pas changée souvent ! En effet, elle a été initialisée à la première cérémonie le 16 juin 2010 (il s'agit d'une paire de clés cryptographiques de 2048 bits, de type RSA), une nouvelle clé a été générée à la cérémonie n°27 le 27 octobre 2016 puis une nouvelle clé sera générée le 27 avril 2023 lors de la cérémonie n°49. Ce n'est donc pas la RKSK qui est changée à chaque cérémonie, mais des ZSK (Zone Signing Keys) : la RKSK est utilisée pour signer ces ZSK qui seront utilisées pendant une période de trois mois pour signer la zone racine DNS. Voir la note 14 pour ceux que ça intéresse.

16 https://www.iana.org/help/tcr-criteria

– le détenteur d'actions de clé de récupération (***Recovery Key Share Holder*** = **RKSH**)

Il garde une carte à puce qui servira en cas de catastrophe (défaillance généralisée des systèmes de production) à déchiffrer les sauvegardes des clés de signature de la zone racine.

Un RKSH n'a pas besoin d'assister à des cérémonies régulières mais doit se préparer à être disponible entre 48 heures et 72 heures après l'annonce d'une crise.

Tous les ans, il doit fournir une preuve qu'il garde en toute sécurité sa carte à puce (par exemple une photographie d'eux-mêmes avec le journal du jour et leur clé, ou encore via une phrase secrète[17]).

– le TCR de sauvegarde (***Backup TCR***)

Ce sont des candidats qui souhaiteraient devenir CO ou RKSH et sont validés par la communauté : si un CO ou RKSH devait démissionner de son rôle (ou décédait), des personnes pré-contrôlées seraient ainsi disponibles pour accéder à ces rôles.

Chaque année, ils réaffirment leur admissibilité et leur disponibilité pour entrer dans un rôle de TCR, au besoin.

Il y a 14 CO – 7 sont affiliés à chaque installation, El Segundo (W) et Culpeper (E) – et 7 RKSH :

| Nom | Nationalité | Rôle | E/W | Depuis |
|---|---|---|---|---|
| Fabian Arbogast | Tanzanie | CO 1 | W | 2015 |
| Ralf Weber | Allemagne | CO 2 | W | 2023 |
| João Luis Silva Damas | Portugal | CO 3 | W | 2010 |
| Carlos Martinez | Uruguay | CO 4 | W | 2010 |
| Ólafur Guðmundsson | Islande | CO 5 | W | 2014 |
| Jorge Etges | Brésil | CO 6 | W | 2022 |
| Subramanian Moonesamy | Maurice | CO 7 | W | 2010 |
| Frederico Neves | Brésil | CO 1 | E | 2010 |
| Pia Gruvö | Suède | CO 2 | E | 2022 |
| Ondřej Filip | République Tchèque | CO 3 | E | 2022 |
| Robert Seastrom | États-Unis | CO 4 | E | 2010 |
| Christopher Griffiths | États-Unis | CO 5 | E | 2013 |
| Gaurab Upadhaya | Népal | CO 6 | E | 2010 |
| Dileepa Lathsara | Sri Lanka | CO 7 | E | 2022 |

Jusqu'à 2014, les TCRs se rendaient à la cérémonie à leurs frais ou à ceux de leur employeur.

Depuis, l'IANA offre[18] une allocation de 300 $, destinée à couvrir les frais (repas, transport, parking, vaccinations, etc.). Si les dépenses engagées sont raisonnables mais supérieures, ils peuvent demander à être remboursées des coûts réels.

| Nom | Nationalité | Rôle | Depuis |
|---|---|---|---|
| Moussa Guebre | Bahamas | RKSH | 2010 |
| David Lawrence | États-Unis | RKSH | 2022 |
| Kristian Ørmen | Danemark | RKSH | 2017 |
| Norm Ritchie | Canada | RKSH | 2010 |
| Ondřej Surý | République Tchèque | RKSH | 2010 |
| Bevil Wooding | Trinité-et-Tobago | RKSH | 2010 |
| Jiankang Yao | Chine | RKSH | 2010 |

**Tous les scénarios ont été pensés, même les plus improbables…**

Et si un événement rendait les HSM inopérants (par exemple, un bug catastrophique dans le firmware) ? L'ICANN conserve une sauvegarde pour chaque clé racine, sous une forme hautement chiffrée, dans un coffre-fort de chaque KMF. Si quelque chose arrivait aux quatre HSM, l'ICANN pourrait acheter un nouveau HSM du même fabricant et restaurer les clés racine à l'aide de la sauvegarde. Dans ce scénario, il faudrait la présence d'au moins 3 RKSH.

17 Source : https://www.iana.org/help/tcr-answers

18 https://www.iana.org/help/tcr-travel-support

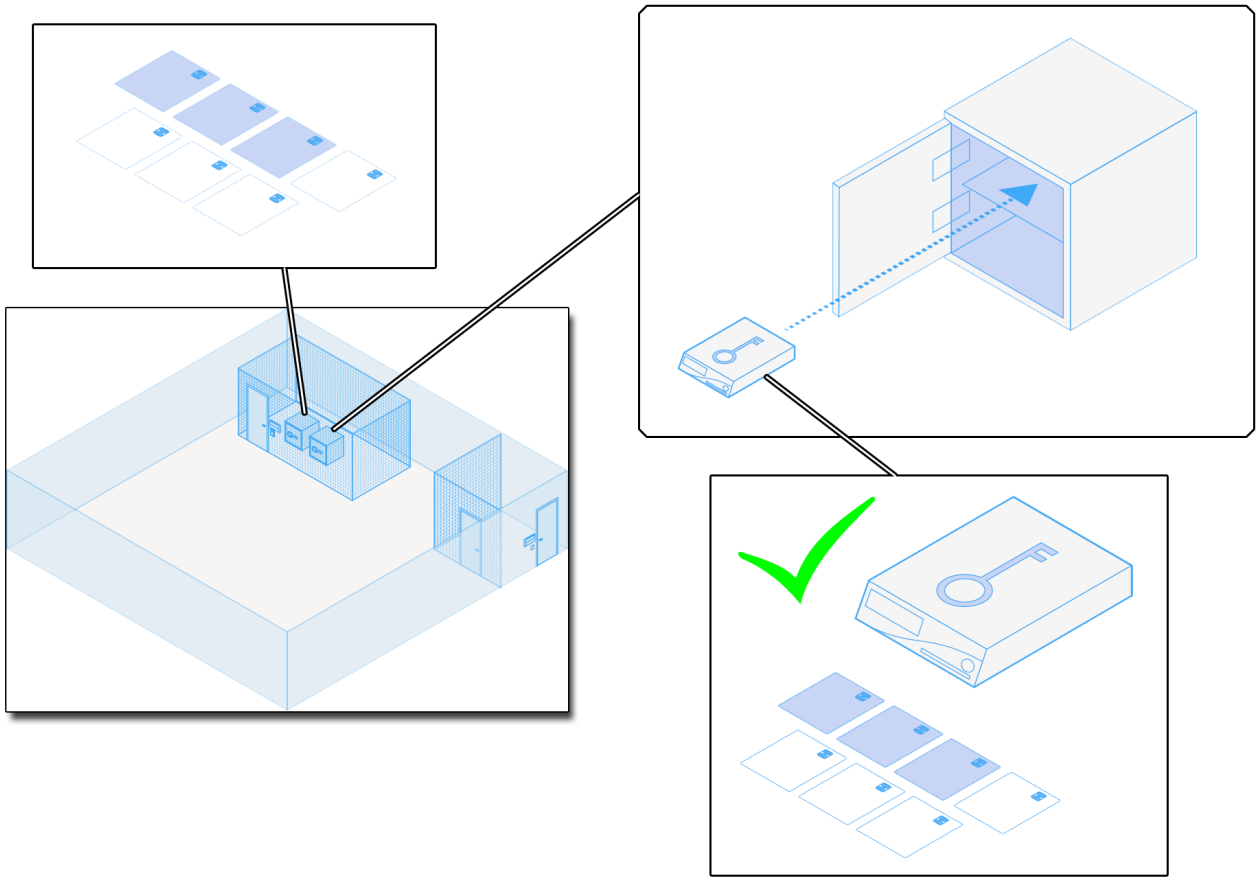
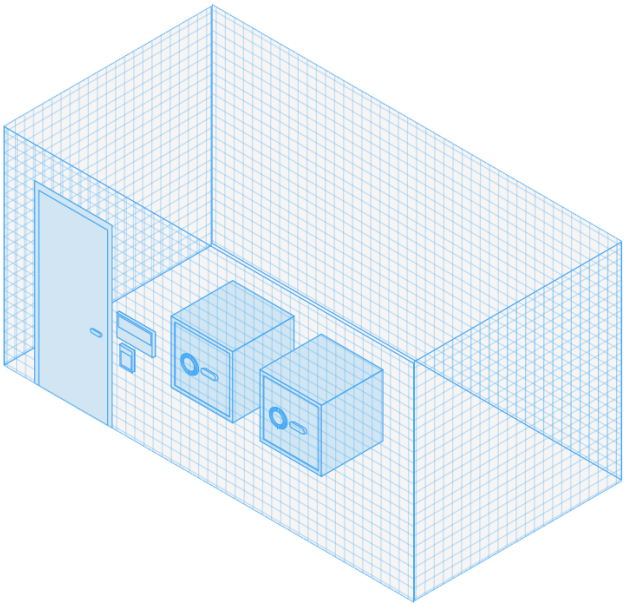


Figure 7: Source des quatre images : PTI/ICANN — Infographie : Johan MATHIEU

Chaque HSM est configuré de telle sorte que **3 des 7 cartes à puces détenues par les CO doivent être présentes** pour le rendre utilisable.

Le HSM est stocké dans un coffre-fort de haute sécurité, qui ne peut être ouvert que par une personne désignée et qui est surveillé avec des capteurs (notamment sismiques !).



Les coffres-forts sont stockés dans une salle sécurisée (*safe room*), qui est en fait une cage qui ne peut être ouverte que conjointement par deux personnes désignées : l'administrateur de la cérémonie et le témoin interne. La salle est surveillée avec des capteurs d'intrusion et de mouvement : en 2014, pendant la cérémonie n°16, un contrôleur de sécurité a claqué une porte sécurisée, déclenchant un capteur sismique qui a déclenché à son tour des verrous de porte… Tous enfermés dans la cage ! Seule solution trouvée : déclencher une alarme et une évacuation, pour reprendre le protocole…

Le coffre-fort est situé dans une pièce plus grande où sont célébrées des cérémonies impliquant les TCR et d'autres personnes. **Les cérémonies sont enregistrées sur vidéo[19], en présence des participants et d'autres personnes, et auditées par un cabinet d'audit tiers.** L'accès à la salle doit être accordé par une autre personne désignée (le responsable du contrôle d'accès physique), qui n'est pas sur place.

19 Pour voir la cérémonie n°48 (du 1er février 2023) et ses documents associés, voir https://www.iana.org/dnssec/ceremonies/48

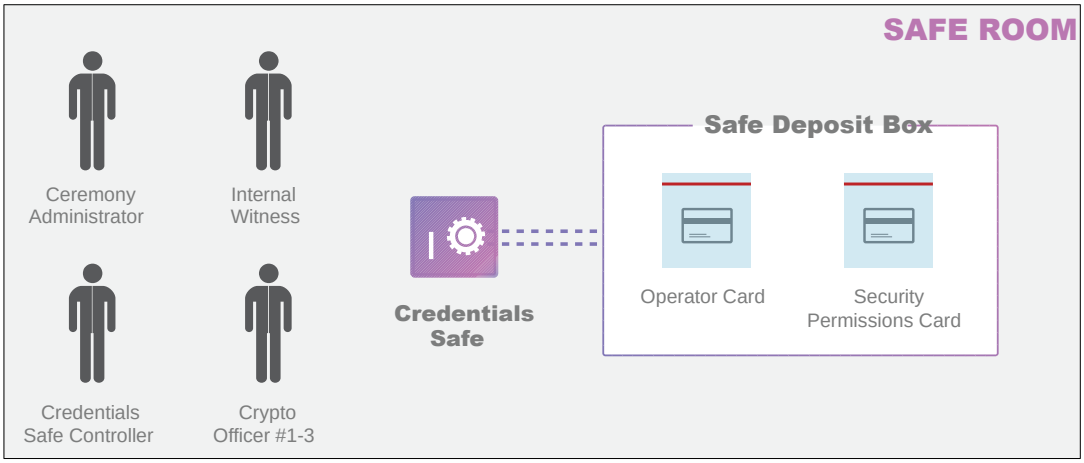
**Les cérémonies de signature des clés sont des événements publics, conçus pour promouvoir la sensibilisation à cet élément de confiance clé pour le système de noms de domaine Internet.**

La date de chaque cérémonie est fixée si possible au moins six mois à l'avance, après avoir sollicité la disponibilité des TCR potentiels et du personnel de la cérémonie.

Globalement, voici le protocole pour arriver jusqu'à la salle de cérémonie :

– pour entrer dans l'établissement, il faut montrer une pièce d'identité délivrée par le gouvernement américain et montrer le contenu de son sac. En retour, on obtient une bande d'identité qu'on colle sur son vêtement. Un membre du personnel de l'ICANN nous escorte alors à l'intérieur (cela nécessite un code PIN, une carte à puce et un scan biométrique de la main)
– arrivée dans une salle de repos où il y a de la nourriture
– lorsque tout le monde est là, les personnes sont escortées – par groupes de 8 maximum – vers une salle d'entrée de la cérémonie : pour y accéder, un membre du personnel de l'ICANN doit utiliser une carte à puce. Dans cette salle d'entrée, chacun signe un journal avant de pouvoir entrer dans la salle de cérémonie principale : pour cela, un scan de la rétine du membre de l'ICANN est nécessaire
– arrivée dans la salle de cérémonie principale : les agents de sécurité de l'immeuble y sont interdits, tout comme les nettoyeurs (c'est un des CO qui est chargé de faire un rapide ménage avec un petit aspirateur).

La salle de cérémonie a une cage sur le côté, qui contient deux coffres-forts : SAFE1 et SAFE2.
Ces coffres-forts stockent tout le matériel sensible utilisé lors de la cérémonie.
Nous allons voir que seules 6 personnes peuvent (et doivent) rentrer dans cette cage.




**La cérémonie est une succession de cinq actes** (durée d'environ trois heures), minutieusement décrits dans un script librement accessible sur le site de l'IANA. Pour plus de détails, voir en annexe.

De nombreux articles parlant des « clés de l'Internet » racontent donc n'importe quoi !
En effet, chacun des 14 détenteurs de clés « primaires » possède une clé métallique traditionnelle qui ouvre un coffre-fort haute-sécurité, qui contient une carte à puce qui permettra d'activer une machine sécurisée (HSM) qui créera une nouvelle clé « principale » pour DNSSEC.
Personne ne garde sur lui et sans aucun contrôle les clés cryptographiques d'un serveur racine.
Il faut bien se rappeler également que ces clés ne sont utiles que pour DNSSEC : Internet est bien plus que ce protocole qui reste tout de même très important, puisqu'il permet de rendre la confiance aux internautes après les failles récentes liées aux DNS.

# → ANNEXE : script général d'une cérémonie[20] des clés ←

## ACTE 1 : lancement de la cérémonie et récupération du matériel

On ne peut entrer dans la cage qu'en présence de l'administrateur de la cérémonie (*Ceremony Administrator* = CA) et d'un témoin interne (*Internal Witness* = IW), qui doivent présenter une carte d'accès et scanner leurs rétines.
Mais aucune de ces deux personnes ne pourra ouvrir un des coffres-forts : il faut pour cela les deux contrôleurs de coffres-forts : SSC1 et SSC2 (*Safe Security Controller* = SSC).
SSC2 ouvre le coffre-fort SAFE2 : il commence par faire tourner rapidement le cadran dans le sens antihoraire afin de le charger, puis rentre la combinaison.


SAFE2 contient un journal de sécurité (*safe log*) c'est-à-dire un classeur de comptes-rendus, qu'il faut remplir (date, signatures de IW et SSC2) et d'autres coffres-forts, chacun nécessitant deux clés : le CA possède l'une de ces clés et chacun des CO a une clé.

L'un après l'autre et avec l'aide de CA, CO1/CO2/CO3 ouvrent leur coffre (*safe deposit box*).
Celui-ci contient deux sacs inviolables (*Tamper Evident Bag* = TEB) qu'on ne peut ouvrir qu'avec des ciseaux : les sacs OP TEB et SO TEB (OP = *operator* et SO = *Security Officer*).
À l'aide d'une lampe de poche, chaque CO vérifie que le coffre ne contient rien d'autre, puis sort les deux TEB. Il lit à voix haute les numéros des TEB (du type # BB46592028 qui se lit « bravo bravo four six five nine … ») en le montrant à la caméra et vérifie que chaque TEB est en bon état (donc ne présente aucune trace d'ouverture, aussi petite soit-elle). Il remet SO TEB dans le coffre[21], mais garde OP TEB, referme le coffre et signe le *safe log*, qui est vérifié par IW (ce sera le cas à chaque étape de la cérémonie).

Chaque anomalie sera mentionnée sur le script, qui sera mis en ligne et librement accessible.

Puis SSC2 remet le *safe log* dans SAFE2 et le verrouille : CA et IW vérifient que le coffre-fort est verrouillé et que le voyant lumineux "WAIT" est éteint.

CA, IW, SSC2 et les trois CO quittent la salle de sécurité avec les OP TEB, fermant la porte derrière eux.
CA et IW prennent un chariot et escortent SSC1 dans la *safe room*.
SSC1 ouvre SAFE1. Il contient :

– deux HSM (HSM1 et HSM2)[22]
– deux ordinateurs portables (LAPTOP1 et LAPTOP2) qui n'ont pas de disque dur
– un DVD contenant un système d'exploitation[23] (OS DVD), chacun dans un sac inviolable (TEB)
– HSM FD : une clé USB qui contient un fichier utile pour le HSM
– KSK-2017 : la RKSK changée à la cérémonie n°27 le 27/10/2016 (voir la note de bas de page n°15).

20 Basé sur la cérémonie 39 du 14 novembre 2019 : https://www.iana.org/dnssec/ceremonies/39.

21 Ce sac contient deux cartes SO CARD qui ne sont utilisées que lorsqu'il faut créer/supprimer des cartes pour les CO (par exemple, lors d'un changement de HSM) ou lorsqu'il faut « transférer la clé de signature racine » (ce qui n'est arrivé que trois fois depuis 2010), c'est pourquoi elles restent souvent dans le coffre.

22 Pour la cérémonie 39, il y a également HSM5E qui a été introduit à la cérémonie 37 et servira aux prochaines cérémonies, en remplaçant d'un ancien HSM.

23 Système d'exploitation : Ceremony Operating ENvironment (COEN). C'est une distribution GNU/Linux (Debian) customisée par l'ICANN, dont le code source est librement accessible sur GitHub.

Le CA sort avec précaution (matériel fragile) chaque équipement, en lisant le numéro du TEB et en vérifiant son intégrité et le montrant à la caméra.
HSM2 / LAPTOP2 retournent dans SAFE1 tandis que HSM1 / LAPTOP1 sont placés sur le chariot.

## ACTE 2 : installation du matériel

Chaque TEB est inspecté, on vérifie son numéro, on l'ouvre et son contenu est placé sur la table de cérémonie, à des emplacements définis à l'avance. Si l'objet placé a un numéro de série, on le vérifie.
CA vérifie que LAPTOP1 ne contient ni disque dur ni batterie.
CA démarre l'ordinateur portable, après y avoir connecté une imprimante par USB et inséré OS DVD.

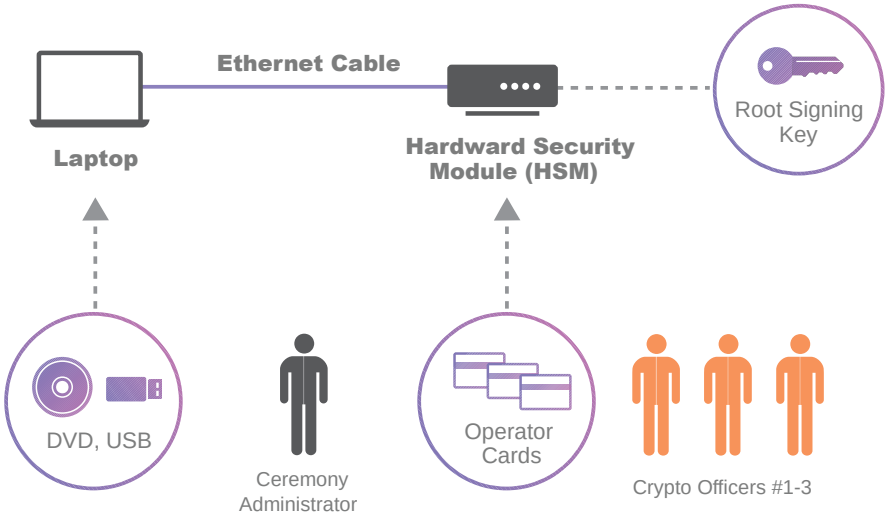



Figure 8: Source : Cloudflare

Le système d'exploitation démarre et il faut configurer l'affichage dupliqué vers un écran visible par tous ceux présents dans la salle de cérémonie (visible sur la vidéo de retransmission sur le Web).

Il faut alors vérifier l'intégrité de l'OS DVD. Pour cela, on fait calculer le *hash* (SHA-256) de l'OS[24]. Ce *hash* est codé en hexadécimal (sur 256 bits, c'est-à-dire 32 octets ; chaque octet est codé par un des $16 \times 16 = 256$ symboles, par exemple b8), soit sous la forme d'un code de 64 caractères :

8105b885b176741d25ef9d391c6a302aed3f6c916093a621a865cb90d560774f.

Or, vérifier une telle succession de lettres/chiffres est fastidieux et peu sécurisé, c'est pourquoi on convertit ce code en une succession de mots de PGP[25] : par exemple, le code hexadécimal 05 correspond au mot *adult* ou *almighty*… Par exemple, le *hash* ci-dessus devient :

> *minnow almighty select leprosy sailboat impetus indoors breakaway bombast unravel quadrant corporate befriend hamburger chairlift chambermaid tunnel customer glucose miracle facial molasses rematch Camelot retouch glossary spheroid millionaire sterling fortitude involve document*

Le CA lit donc chaque mot : IW et tous les participants en vérifient l'exactitude.
Il faut ensuite :

– configurer l'imprimante
– régler l'heure et la date[26] (en utilisant celle affichée sur l'horloge de la pièce)
– dans LAPTOP1, on insère une clé USB qui contient un fichier qui servira au HSM1, et on vérifie son *hash*
– on relie[27] HSM1 à LAPTOP1 et on allume HSM1 (cela affiche des informations : on vérifie le numéro de série du HSM1).

24 Image ISO.

25 Pour ceux que ça intéresse, voir https://fr.wikipedia.org/wiki/Liste_de_mots_de_PGP.

26 C'est la même horloge utilisée depuis la première cérémonie, et elle est complètement isolée du reste du monde. Elle a légèrement dérivé, mais c'est très bien, car elle n'est utilisée qu'à des fins de journalisation. (source : Cloudflare)

27 Via un *null modem cable*.

## ACTE 3 : activer HSM1 et générer les signatures

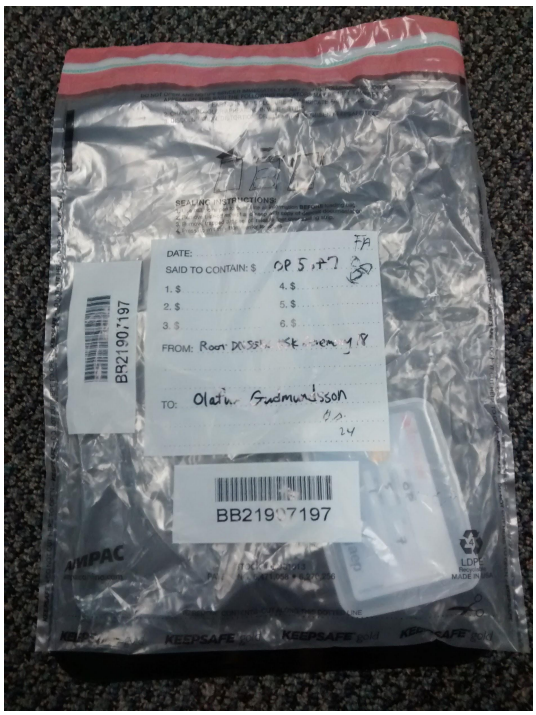


Figure 9: Source : Cloudflare

Pour chacun des trois CO et pour chaque OP TEB :
a) CO lit à haute voix le numéro du TEB, puis CA l'inspecte pour détecter toute falsification.
b) CO et CA ouvrent le TEB, qui contient un boîtier en plastique contenant une carte à puce[28] OP CARD.
Les étuis en plastique sont importants, car quelqu'un a découvert qu'il était possible de manipuler les cartes en passant des aiguilles dans le sac inviolable, ce qui ne serait pas nécessairement perceptible lors de l'inspection du sac[29].
c) CA ouvre ce boîtier, puis place la carte située à l'intérieur sur le porte-cartes à l'avant de la table de cérémonie.

On active le HSM1 en y entrant successivement les trois OP CARD avant de taper le code PIN 11223344.
Par câble ethernet, on relie LAPTOP1 à HSM1, et on vérifie que le réseau fonctionne.
On insère une clé USB (KSR FD) qui contient les demandes de signatures de clés (*Key Signing Request* = KSR).
On lance une application[30] qui utilise la clé privée stockée dans HSM1 pour générer les signatures de clés[31] (*Signed Key Response* = SKR) qui seront utilisées au cours du prochain trimestre.
On calcule le *hash* du fichier ainsi créé (qui contient les signatures) : un employé de Verisign (nommé RZM pour *Root Zone Maintainer*) lit la liste des mots de PGP représentant ce *hash*, et tout le monde en vérifie l'exactitude.
On copie le fichier créé sur le HSM1. La clé USB KSR FD est rendue à l'employé ci-dessus.
On désactive HSM1 (encore à l'aide des trois cartes à puces OP CARD), puis on le place dans un nouveau TEB que l'on ferme : CA lit le numéro TEB ainsi que le numéro de série du HSM1, et montre le TEB ainsi créé à la caméra. CA pose ce TEB sur le chariot.

## ACTE 4 : mettre à jour et sécuriser le matériel

Le CA sauvegarde sur 4 clés USB (neuves et formatées pendant la cérémonie) le contenu de HSM FD : deux clés pour IW (qui seront auditées) et deux qui seront remises au RZM puis analysées.
CA imprime le journal (*log* consultable sur le Web) des actions effectuées.
CA déconnecte les équipements, imprime sur une feuille de papier le *hash* du HSM FD et les replace à l'intérieur de nouveaux TEB qu'il faut vérifier.
CA et IW escortent SSC1 pour remettre les équipements dans SAFE1.
CA et IW escortent SSC2 et les trois CO pour remettre les cartes à puce dans SAFE2.

## ACTE 5 : clôture de la cérémonie

CA relit toutes les anomalies notées pendant la cérémonie.
Toutes les personnes présentes viennent signer le script, et ainsi déclarent qu'il est valide.

28 Dès la cérémonie n°45, il semble que deux OP CARD soient utilisées.
29 https://www.cloudflare.com/dns/dnssec/root-signing-ceremony/
30 Dont le code source est disponible : https://github.com/iana-org/dnssec-keytools.
31 Les *Zone Security Keys* = ZSKs

On arrête la diffusion (streaming) en direct.
CA informe les participants de la suite des activités (une petite fête ?) et une photo de groupe est prise.

Figure 10: Photo de la cérémonie n°38 du 14 août 2019

CA veille à ce que tous les participants soient escortés hors de la salle de cérémonie des clés, mais aussi qu'ils ne peuvent plus y entrer (badges déconnectés), sauf IW, le *System Administrator* et lui qui y restent.
CA demande alors à ce que l'enregistrement vidéo soit arrêté.
En effet, tout est enregistré même après l'arrêt de la diffusion en direct, car tout sera audité par un organisme.